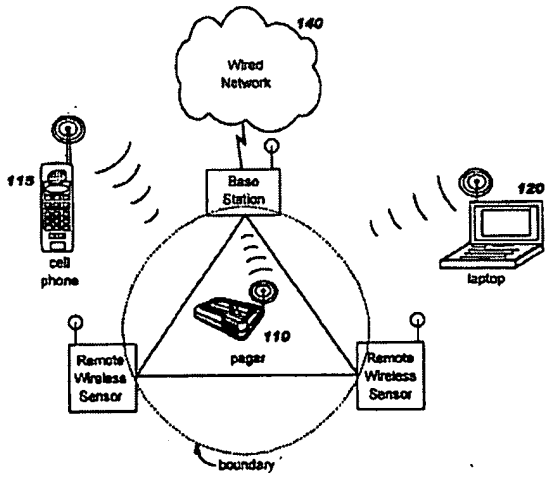
REMARKS

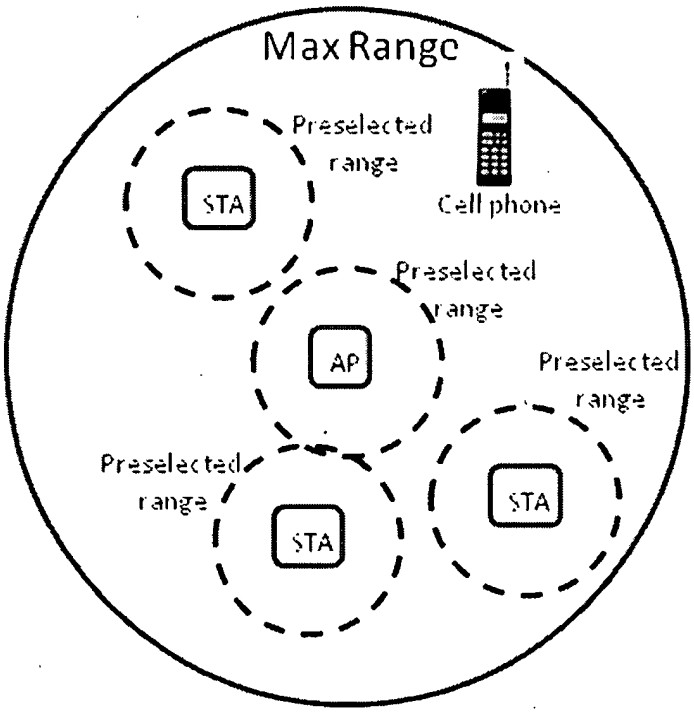
Claims 1-18 are pending in this application. All of the pending claims are rejected. None of the claims are currently amended. Reconsideration and further examination are respectfully requested.

Claims 1-2, 4-8, 10-15, and 17-18 are rejected under 35 U.S.C. 102(e) as being anticipated by US 7,212,828 (Hind). With regard to independent claims 1, 11, 17 and 18, the examiner cites Hind at column 2, between lines 38 and 62. In the passage cited by the examiner and elsewhere Hind describes establishment of a spatial boundary defined around a WiFi network. Client devices outside the boundary may be denied access. However, Hind's boundary is not equivalent to the range recited in the claims. For example, Hind defines only one boundary for a BSS, the boundary is not centered on a particular device, and the boundary is not limited in any way by the maximum communication range of the network. Rather, Hind's boundary is an area defined by remote wireless sensors as shown in figure 3 of Hind, depicted below.

FIG. 3



In contrast with the boundary defined by Hind, the preselected range recited in the independent claims is defined relative to a network device, and is less than the maximum communication range of the network. Because the range is defined by distance to a network device, there can be multiple authentication zones, and those zones are centered on devices. Further, the range must be less than the maximum range of the network, which is defined by the location and power of the access point or base station. The following figure illustrates an example of these limitations.



Note that the cell phone is denied authentication because it is not within a preselected range of a network device, even though it is within maximum range of the network, i.e., within range of the AP. An advantage of the recited technique is that network devices tend to be located within a

confined work area, and a rogue device located near to one of those devices, i.e., within the work area, is more likely to be a legitimate user than a rogue device located far away from those devices, i.e., outside the work area. Note that rather than having to define a boundary with specialized sensors as in Hind, the presently claimed invention automatically defines an area based on the locations of devices that are already authenticated. The examiner attempts to equate Hind's boundary with both the preselected range and the maximum communication range, but this is not logical because the recited limitation is that the preselected range is less than the maximum range, not less than or equal. Because Hind fails to anticipate either authentication based on distance to a network device or authentication based on distance relative to maximum communication range, the rejections should be withdrawn.

The dependent claims further distinguish the invention, and are allowable for the same reasons as their respective base claims. With regard to claim 10, which recites determining distance from signal strength, note that Hind expressly dismisses this technique at column 4, lines 22-23, stating "the signal strength seen at a receiver is of no use in determining the distance to the transmitter." With regard to claims 3, 9 and 16, the examiner concedes that Hind fails to disclose the recited features but nevertheless asserts that the features are obvious. Applicant requests that an actual prior art reference be provided showing the features.

Respectfully Submitted,

October 20, 2008
Date

/Holmes W. Anderson/
Holmes W. Anderson, Reg. No. 37,272
Attorney/Agent for Applicant(s)
Anderson Gorecki & Manaras LLP
33 Nagog Park
Acton, MA 01720
(978) 264-4001

Docket No. 160-068
Dd: 10/16/2008